PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-358717
(43)Date of publication of application : 26.12.2001

(51)Int.Cl. H04L 12/24
H04L 12/26
G06F 13/00
G06F 15/00
H04L 12/46
H04L 12/28
H04L 12/56
// G06F 17/60

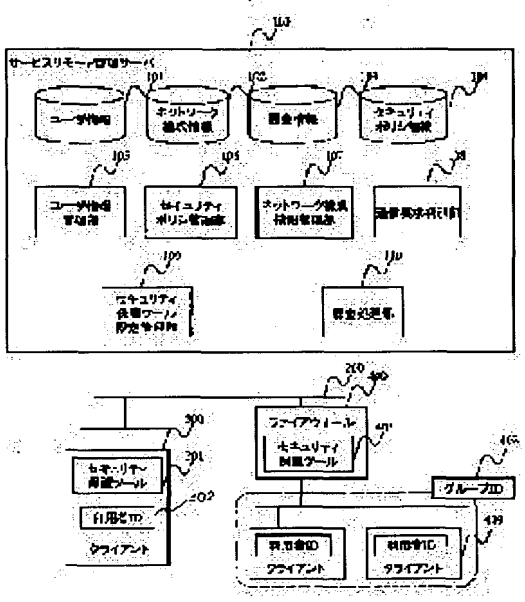
(21)Application number : 2000-175815
(22)Date of filing : 12.06.2000

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : FUJI HITOSHI

(54) METHOD AND DEVICE FOR MANAGING NETWORK DEVICE OR THE LIKE AND PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To allow a side entrusted with the management of a network, device, software, etc., to perform entrusted work and to obtain a remuneration from an entrusting side.
SOLUTION: In this method for managing the network device, etc., a network user transmits a communication request to a managing device such as the network device via a network, the managing device receives the communication request, changes the settings of network device software, etc., needed to meet the communication request on the basis of the received communication request, performs communication request reflection processing on the basis of a user ID or group ID attached to the communication request, performs the request reflection processing as it is in the case of a system according to weight, delivers the network device, the software, etc., whose setting has to be changed to meet the communication request from network configuration information, gives a setting change instruction to the network device, the software, etc., when the communication request coincides with a security policy or when the security policy is not checked, and performs to filling after performing a series of these pieces of processing when the user who has transmitted the communication request selects charging based on the system according to weight.

図 1



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－358717
（P2001－358717A）
(43)公開日　平成13年12月26日(2001.12.26)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
H04L	12/24		G06F	13/00	530S	5B049
	12/26			15/00	330Z	5B085
G06F	13/00	530		17/60	332	5K030
	15/00	330	H04L	11/08		5K033
H04L	12/46			11/00	310C	

審査請求　未請求　請求項の数12　ＯＬ　（全 17 頁）　最終頁に続く

(21)出願番号　特願2000－175815(P2000－175815)

(22)出願日　平成12年６月12日(2000.6.12)

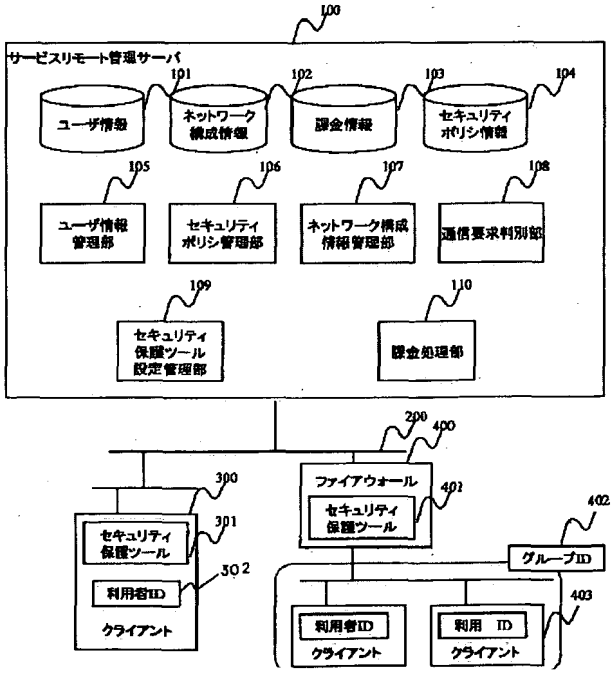
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　冨士　仁
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083552
弁理士　秋田　収喜

Ｆターム(参考)　5B049 AA06 CC36 GG04 GG07
5B085 AC04 AE02 BG07
5K030 GA15 HA08 JA10 KA01 KA07 KA13
5K033 AA08 CC01 DA01 DB14 DB20 EA07

(54)【発明の名称】　ネットワーク機器等の管理方法及び装置ならびにプログラムの記録媒体

(57)【要約】
【課題】　ネットワーク機器、ソフトウェア等の管理を委託された側で委託した作業を行い、委託した側から対価を得る。
【解決手段】　ネットワーク利用者が、通信要求をネットワーク経由でネットワーク機器等の管理装置に送信し、通信要求を管理装置が受信し、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更し、通信要求に付与されている利用者ＩＤ又はグループＩＤに基づいて通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行い、通信要求がセキュリティポリシに合致しているとき、又はセキュリティポリシのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出し、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行うネ

図１



【特許請求の範囲】

【請求項１】　ネットワークの管理を実施するユーザネットワーク機器、ソフトウェア等の設定変更を必要とするユーザのセキュリティポリシのチェックを、マネージドサービスプロバイダ側で実施するようにすることを特徴とするネットワーク機器等の管理方法。

【請求項２】　ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等の管理装置（以下、管理装置と称する）に送信し、前記通信要求を管理装置が受信し、前記通信要求に付与されている利用者ＩＤ又はグループＩＤに基づいて通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行い、前記通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行うことを特徴とするネットワーク機器等の管理方法。

【請求項３】　ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等の管理装置（以下、管理装置と称する）に送信し、前記通信要求を管理装置が受信し、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更し、前記ネットワーク利用者が管理装置に送る通信要求には、利用者ＩＤ又はグループＩＤを付与し、前記管理装置では、送信されてきた利用者ＩＤ又はグループＩＤを識別し、それらのＩＤが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックし、権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックし、滞納がなければ、次の通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行い、前記通信要求反映処理では、通信要求の内容を解析し、その通信要求が管理装置に登録されている通信要求を送信した利用者もしくは利用者が属しているグループのセキュリティポリシに合致しているか否かのチェックを行い、前記通信要求がセキュリティポリシに合致しているとき、又はセキュリティポリシのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出し、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行い、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行うことを特徴とするネットワーク機器等の管理方法。

【請求項４】　請求項２又は３に記載のネットワーク機器等の管理方法において、前記管理装置には、新規の利用者の登録及び課金情報について登録されることを特徴とするネットワーク機器等の管理方法。

【請求項５】　請求項４に記載のネットワーク機器等の管理方法において、前記課金情報には、課金方法、決済方法などが含まれ、課金方法は、ネットワーク利用者単位、又はネットワーク利用者が属するグループ単位に、従量制課金又は定額制課金を選択可能とすることを特徴とするネットワーク機器等の管理方法。

【請求項６】　請求項５に記載のネットワーク機器等の管理方法において、ネットワーク利用者単位又はグループ単位での課金は、ネットワーク利用者が通信要求を管理装置に送信するたびに、そのネットワーク利用者が事前に登録している決済方法に対して請求処理を行うことを特徴とするネットワーク機器等の管理方法。

【請求項７】　請求項６に記載のネットワーク機器等の管理方法において、前記請求処理が、従量制課金の場合には、ネットワーク利用者の通信要求が送信されるたびに、ある金額の請求が加算される形で行われ、定額制課金の場合には、ネットワーク利用者の通信要求が送信されるときに定額制課金であるかが確認されることを特徴とするネットワーク機器等の管理方法。

【請求項８】　請求項２乃至７のうちいずれか１項に記載のネットワーク機器等の管理方法において、前記管理装置では、送信されてきた利用者ＩＤ又はグループＩＤを識別し、それらのＩＤが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックし、権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックし、滞納がなければ、通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行うことを特徴とするネットワーク機器等の管理方法。

【請求項９】　ネットワーク機器等の管理方法の処理手順を、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であって、ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等の管理装置（以下、管理装置と称する）に送信する手順と、前記通信要求を管理装置が受信する手順と、前記通信要求に付与されている利用者ＩＤ又はグループＩＤに基づいて通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行う手順と、前記通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行う手順とを、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１０】　ネットワーク機器等の管理方法の処理手順を、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であって、ネットワーク利用者が、論理閉域網を生成、変更、又は削除

するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等の管理装置（以下、管理装置と称する）に送信する手順と、前記通信要求を管理装置が受信する手順と、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更する手順と、前記ネットワーク利用者が管理装置に送る通信要求には、利用者ＩＤ又はグループＩＤを付与する手順と、前記管理装置では、送信されてきた利用者ＩＤ又はグループＩＤを識別する手順と、それらのＩＤが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックする手順と、権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックする手順と、滞納がなければ、次の通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行う手順と、前記通信要求反映処理では、通信要求の内容を解析し、その通信要求が管理装置に登録されている通信要求を送信した利用者もしくは利用者が属しているグループのセキュリティポリシに合致しているか否かのチェックを行う手順と、前記通信要求がセキュリティポリシに合致しているとき、又はセキュリティポリシのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出する手順と、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行う手順とを、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１１】　サービスリモート管理サーバと、前記サービスリモート管理サーバとネットワーク利用者が使用中のネットワークを結ぶネットワーク（例えばインタネット）と、ネットワーク利用者が使用中のネットワークと外部のネットワークとの接続を制御しているファイアウォールとを有するネットワーク機器等の管理装置において、サービスリモート管理サーバが、利用者の情報を記録（保存）しているユーザ情報データベースと、ネットワーク構成情報を保存しているネットワーク構成情報データベースと、課金方法、決済方法及びサービスに対する課金の情報を記録（保存）している課金情報データベースと、ネットワーク利用者から送信されてきた通信要求の可否を判別する通信要求判別部と、通信要求を満たすために必要な具体的なネットワーク機器等の設定を導出するセキュリティ保護ツール設定導出部と、ネットワーク利用者の使っているネットワークの情報を管理しているネットワーク構成情報管理部と、ネットワーク利用者から通信要求が送られて来たときに課金処理を行う課金処理部とを有することを特徴とするネットワーク機器等の管理装置。

【請求項１２】　請求項１１に記載のネットワーク機器等の管理装置において、前記セキュリティ保護ツール設定導出部は、利用者が登録情報をユーザ情報管理部に送信する手段と、前記送信された登録情報をユーザ情報データベース（利用者登録データベース）に記録（保存）する手段と、利用者登録が済んでからセキュリティポリシをセキュリティポリシ管理部に送信する手段と、セキュリティポリシ情報データベースに登録する手段と、ネットワーク利用者から通信要求を受け付ける手段と、前記受け付けられた通信要求に基づくセキュリティポリシの変更処理を行う手段とを有することを特徴とするネットワーク機器等の管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワーク機器、ソフトウェア等の管理をマネージドサービスプロバイダと呼ばれる外部組織に委託することに関し、特に、ネットワーク利用者が論理閉域網を要求してから、人による作業を介することなく、論理閉域を使えるようにすると共に、ネットワーク機器、ソフトウェア等の管理を委託された側で委託した作業を行い、委託した側から対価を得る方法及び装置に適用して有効な技術に関するものである。

【０００２】

【従来の技術】ネットワーク機器、ソフトウェア等のネットワーク管理をマネージドサービスプロバイダと呼ばれる外部組織、企業など（以下、ＭＳＰと称する）にアウトソーシングすることが行われている。これは、ある物理ネットワークに接続されているネットワーク機器、ソフトウェア等、又はある物理ネットワークと専用線などの他者と共有しないネットワークで接続されている別の物理ネットワークに設置されているある物理ネットワークの接続に使われているネットワーク機器、ソフトウェア等を、ＭＳＰがそのネットワークの所有者の要望に沿った方針で管理することによって、管理の対価を得るサービスとして行われている。

【０００３】

【発明が解決しようとする課題】しかしながら、前記ＭＳＰによるネットワーク機器等の管理サービスでは、ネットワーク機器を経由する他ネットワークとの接続方針の決定は、ネットワークの所有者（個人又は組織）にあり、その方針又は具体的なネットワーク機器等の設定内容をＭＳＰに伝えることによって、方針が伝えられたときにはＭＳＰがネットワーク機器固有の設定情報に変換し、ネットワーク機器の設定内容が伝えられたときにはその内容を使い、ネットワーク機器の設定を行う。

【０００４】このネットワークの所有者からＭＳＰへ伝えられた方針又は設定情報は、ネットワーク所有者が保持しているセキュリティポリシに合致していることが求

められる。このため内容のチェックが行われるのが普通で、ネットワークの所有者が行うか、チェック自体もＭＳＰによって行われる。

【０００５】このようなチェックは、これまで人の手を介するしか方法がなかったため、ネットワーク利用者の通信要求は、ネットワークの所有者、その所有者から委託されたネットワーク管理者、又はその利用者からＭＳＰによってチェックされていた。

【０００６】そこで、ネットワーク利用者の通信要求等のチェックを、人の手を介することなくＭＳＰ側で行うことできるようにすることが要望されている。

【０００７】本発明の目的は、ネットワーク機器、ソフトウェア等の管理を行うネットワーク機器等の管理方法及び装置において、ネットワーク機器、ソフトウェア等の管理を委託された側で委託した作業を行い、委託した側から対価を得ることが可能な技術を提供することにある。

【０００８】本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかにする。

【０００９】

【課題を解決するための手段】本願において開示される発明の概要を簡単に説明すれば、下記のとおりである。

【００１０】（１）ネットワークの管理を実施するユーザネットワーク機器、ソフトウェア等の設定変更を必要とするユーザのセキュリティポリシのチェックを、マネージドサービスプロバイダ側で実施するようにするネットワーク機器等の管理方法である。

【００１１】（２）ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等管理装置（以下、管理装置と称する）に送信し、前記通信要求を管理装置が受信し、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更し、前記通信要求に付与されている利用者ＩＤ又はグループＩＤに基づいて通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行い、前記通信要求がセキュリティポリシに合致しているとき、又はセキュリティポリシのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出し、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行うネットワーク機器等の管理方法である。

【００１２】（３）ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等管理装置（以下、管理装置と称する）に送信し、前記通信要求を管理装置が受信し、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更し、前記ネットワーク利用者が管理装置に送る通信要求には、利用者ＩＤ又はグループＩＤを付与し、前記管理装置では、送信されてきた利用者ＩＤ又はグループＩＤを識別し、それらのＩＤが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックし、権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックし、滞納がなければ、次の通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行い、前記通信要求反映処理では、通信要求の内容を解析し、その通信要求が管理装置に登録されている通信要求を送信した利用者もしくは利用者が属しているグループのセキュリティポリシに合致しているか否かのチェックを行い、前記通信要求がセキュリティポリシに合致しているとき、又はセキュリティポリシのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出し、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行うネットワーク機器等の管理方法である。

【００１３】（４）前記手段（２）又は（３）のネットワーク機器等の管理方法において、前記管理装置には、新規の利用者の登録及び課金情報について登録されるものである。

【００１４】（５）前記手段（４）のネットワーク機器等の管理方法において、前記課金情報には，課金方法，決済方法などが含まれ、課金方法は、ネットワーク利用者単位、又はネットワーク利用者が属するグループ単位に、従量制課金又は定額制課金を選択可能とするものである。

【００１５】（６）前記手段（５）のネットワーク機器等の管理方法において、ネットワーク利用者単位又はグループ単位での課金は、ネットワーク利用者が通信要求を管理装置に送信するたびに、そのネットワーク利用者が事前に登録している決済方法に対して請求処理を行うものである。

【００１６】（７）前記手段（６）のネットワーク機器等の管理方法において、前記請求処理が、従量制課金の場合には、ネットワーク利用者の通信要求が送信されるたびに、ある金額の請求が加算される形で行われ、定額制課金の場合には、ネットワーク利用者の通信要求が送信されるときに定額制課金であるかが確認される。

【００１７】（８）前記手段（２）乃至（７）のうちい

ずれか１つのネットワーク機器等の管理方法において、前記管理装置では、送信されてきた利用者ＩＤ又はグループＩＤを識別し、それらのＩＤが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックし、権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックし、滞納がなければ、通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行うものである。

【００１８】（９）ネットワーク機器等の管理方法の処理手順を、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であって、ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等管理装置（以下、管理装置と称する）に送信する手順と、前記通信要求を管理装置が受信する手順と、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更する手順と、前記通信要求に付与されている利用者ＩＤ又はグループＩＤに基づいて通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行う手順と、前記通信要求がセキュリティポリシに合致しているとき、又はセキュリティポリシのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出する順と、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行う手順とを、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００１９】（１０）ネットワーク機器等の管理方法の処理手順を、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であって、ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器、ソフトウェア等の設定を変更する通信要求をネットワーク経由でネットワーク機器等管理装置（以下、管理装置と称する）に送信する手順と、前記通信要求を管理装置が受信する手順と、受信した通信要求に基づいて管理装置が通信要求を満たすために必要なネットワーク機器ソフトウェア等の設定を変更する手順と、前記ネットワーク利用者が管理装置に送る通信要求には、利用者ＩＤ又はグループＩＤを付与する手順と、前記管理装置では、送信されてきた利用者ＩＤ又はグループＩＤを識別する手順と、それらのＩＤが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックする手順と、権限がある場合には、通信要求を送信した利用者又はグループがないことをチェックする手順と、滞納がなければ、次の通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行う手順と、前記通信要求反映処理では、通信要求の内容を解析し、その通信要求が管理装置に登録されている通信要求を送信した利用者もしくは利用者が属しているグループのセキュリティポリシに合致しているか否かのチェックを行う手順と、前記通信要求がセキュリティポリシに合致しているとき、又はセキュリティポリシのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器、ソフトウェア等を導出する手順と、該当するネットワーク機器、ソフトウェア等に設定変更指示を与え、これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行う手順とを、コンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【００２０】（１１）サービスリモート管理サーバと、前記サービスリモート管理サーバとネットワーク利用者が使用中のネットワークを結ぶネットワーク（インタネットワーク）と、ネットワーク利用者が使用中のネットワークと外部のネットワークとの接続を制御しているファイアウォールとを有するネットワーク機器等の管理装置において、サービスリモート管理サーバが、利用者の情報を保存しているユーザ情報データベースと、ネットワーク構成情報を保存しているネットワーク構成情報データベースと、課金方法、決済方法及びサービスに対する課金の情報を保存している課金情報データベースと、ネットワーク利用者から送信されてきた通信要求の可否を判別する通信要求判別部と、通信要求を満たすために必要な具体的なネットワーク機器等の設定を導出するセキュリティ保護ツール設定導出部と、ネットワーク利用者の使っているネットワークの情報を管理しているネットワーク構成情報管理部と、ネットワーク利用者から通信要求が送られて来たときに課金処理を行う課金処理部とを有するものである。

【００２１】（１２）前記手段（１１）のネットワーク機器等の管理装置において、前記セキュリティ保護ツール設定導出部は、利用者が登録情報をユーザ情報管理部に送信する手段と、前記送信された登録情報をユーザ情報データベース（利用者登録データベース）に保存する手段と、利用者登録が済んでからセキュリティポリシをセキュリティポリシ管理部に送信する手段と、セキュリティポリシ情報データベースに登録する手段と、ネットワーク利用者から通信要求を受け付ける手段と、前記受け付けられた通信要求に基づくセキュリティポリシの変更処理を行う手段とを有するものである。

【００２２】すなわち、本発明のポイントは、ネットワーク利用者が、論理閉域網を生成、変更、又は削除するようなネットワーク機器の設定を変更する要求をネット

ワーク経由で送信し、その通信要求をネットワーク機器等の管理装置（ＭＳＰ側の管理装置）が受信し、受信した通信要求に基づいて前記ネットワーク機器等の管理装置（以下、単に管理装置と称する）が通信要求を満たすために必要なネットワーク機器、ソフトウェア等の設定を変更する。

【００２３】このために、前記管理装置に通信要求を送るネットワーク利用者には、その利用者を一意に識別できる利用者ＩＤを付与する。この利用者ＩＤは、その利用者を含む一人以上が属するグループを一意に識別できるグループＩＤと関連付け、利用者ＩＤからグループＩＤが導出できるような関係を明確にする。これらのＩＤ付与と関連付けは、新規の利用者が前記管理装置に利用者登録する際に行われる。また、この利用者登録の際に、課金情報についても登録する。

【００２４】課金情報には、課金方法、決済方法などが含まれる。課金方法は、ネットワーク利用者単位、又はネットワーク利用者が属するグループ単位に、従量制課金又は定額制課金を選択可能とする。ネットワーク利用者単位での課金は、ネットワーク利用者が通信要求を前記管理装置に送信するたびに、そのネットワーク利用者が事前に登録している決済方法に対して請求処理を行い、グループ単位の課金では、ネットワーク利用者が通信要求を前記管理装置に送信するたびに、そのネットワーク利用者が属するグループが事前に登録している決済方法に対して請求処理を行う。この請求処理が、従量制課金の場合には、、ネットワーク利用者の通信要求が送信されるたびに、ある金額の請求が加算される形で行われ、定額制課金の場合には、ネットワーク利用者の通信要求が送信されるときに定額制課金であることが確認される。

【００２５】ネットワーク利用者が前記管理装置に送る通信要求には、利用者ＩＤ又はグループＩＤを付与する。どの情報を付与するかは、ＭＳＰが実施する課金方法又はＭＳＰがネットワーク利用者単位課金もグループ単位課金も実施している場合には利用者が選択した課金方法とその管理装置が採用しているＩＤ体系に関わる。

【００２６】前記管理装置では、送信されてきた利用者ＩＤ又はグループＩＤを識別し、それらのＩＤが付与されている利用者又はグループに通信要求を送出する権限があるか否かをチェックする。

【００２７】権限がある場合には、通信要求を送信した利用者又はグループが選択している課金方法を調べ、定額制の場合には滞納がないことをチェックし、滞納がなければ、次の通信要求反映処理を行い、従量制の場合はそのまま要求反映処理を行う。

【００２８】前記通信要求反映処理では、通信要求の内容を解析し、その通信要求が前記管理装置に登録されている通信要求を送信した利用者もしくは利用者が属してかのチェックを行う。セキュリティポリシとのチェックを行い、かつ通信要求がセキュリティポリシに合致しているとき、又はセキュリティポリシのチェックを行わないとき、ネットワーク構成情報から通信要求を満たすために設定を変更する必要があるネットワーク機器等を導出し、該当するネットワーク機器、ソフトウェア等に設定変更指示を与える。これら一連の処理を行った後に、通信要求を送信してきた利用者が従量制課金を選択している場合には、課金処理を行う。

【００２９】前記手段によれば、ネットワーク利用者が論理閉域網を要求してから、人による作業を介することなく、論理閉域を使えるようになる。これにより、従来の人を介した論理閉域網の管理サービスに比べて時間を短縮することができる。

【００３０】また、包含関係ＩＤを利用することによって、サービス提供側で利用者ＩＤとグループＩＤというような複数種類のＩＤの対応関係を表す情報を保持する必要がなくなる。

【００３１】また、ネットワーク機器、ソフトウェア等の管理を行うネットワーク機器等の管理方法及び装置において、ネットワーク機器、ソフトウェア等の管理を委託された側で委託した作業を行い、委託した側から対価を得ることができる。

【００３２】以下に、本発明について、本発明による実施形態（実施例）とともに図面を参照して詳細に説明する。

【００３３】

【発明の実施の形態】まず、本発明に係るセキュリティポリシ管理方法及び装置の実施形態について説明する。

【００３４】図２は、本発明に係る一実施形態のコンピュータシステムからなるセキュリティポリシ管理装置の概略構成を示す模式図である。図２において、１１はネットワーク利用者からの通信要求を受け付ける第１のインタフェース、１２はネットワーク管理者がセキュリティポリシを管理する第２のインタフェース、１３はセキュリティポリシ管理装置からネットワーク機器等に設定を行う第３のインタフェース、１４は他セキュリティポリシ管理装置へのセキュリティポリシ登録を行うセキュリティポリシ連結部、２１はネットワーク利用者からの通信要求をチェックする通信要求チェック部、２２は通信要求を実現するために使える手段を検索する論理閉域網生成手段検索部、２３は論理閉域網生成手段検索部２２で複数の結果が検索された場合に一つの手段を選択する論理閉域網生成手段選択機構部、２４は論理閉域網生成手段選択機構部２３の結果に基づいて現在のネットワーク機器、ソフトウェア等に設定されている状態をチェックするセキュリティ保護ツール設定チェック部（ネットワーク機器設定チェック部）である。

【００３５】３０はセキュリティポリシを保存しているセキュリティポリシデータベース（データベース部）で

あり、このセキュリティポリシデータベース３０には、論理閉域網の状態を管理する論理閉域網構成要素管理部３１、ネットワーク管理者によって管理されているセキュリティポリシ構成要素管理機構部３２、及びセキュリティ保護ツールの状態を管理しているセキュリティ保護ツール構成要素管理部３３を有している。

【００３６】図３は、本実施形態のセキュリティポリシ管理装置の動作手順を示す流れ図である。まず、ネットワーク管理者が管理対象範囲のセキュリティポリシを決め、それをセキュリティポリシ管理装置に登録する（Ｓ３１）。このセキュリティポリシは必要に応じて、ネットワーク管理者が追加、修正、又は削除することができる。この状態以降は、ネットワーク利用者による通信要求を受け付け（Ｓ３２）、それをネットワーク機器等に設定することによって（Ｓ３３）、ネットワーク利用者の要求する通信を実現する。

【００３７】図４は、前記図２に示すセキュリティポリシ管理装置の動作手順の最初であるネットワーク管理者によるセキュリティポリシ管理の処理手順を示す流れ図である。第２のインターフェース（セキュリティポリシ管理インタフェース）１２から入力されたセキュリティポリシは、図４に示すように、追加、変更、又は削除の処理が行われ（Ｓ４１、Ｓ４２、Ｓ４３）、その結果は、セキュリティポリシ構成要素管理部３２に保存される（Ｓ４４）。

【００３８】図５は、セキュリティポリシ管理装置の動作手順（図３）のネットワーク利用者による通信要求処理と、セキュリティポリシ管理装置による機器設定処理の両者に関わる処理手順を示している。これらの処理は、ネットワーク利用者の通信要求が、第１のインターフェース（ユーザ要求インタフェース）１１から入力されたことにより削除の場合は、通信要求チェック部２１は、要求時点に存在している論理閉域網の情報を論理閉域網構成要素管理部３１から得る。

【００３９】図５に示すように、入力された通信要求が、要求を受け付けたセキュリティポリシ管理装置１０００の管理対象範囲内の要求か、他セキュリティポリシ管理装置２０００の管理対象範囲に属する機器との通信が含まれるかという管理対象チェックを、通信要求チェック部２１が、セキュリティポリシ構成要素管理部３２に対して行う（Ｓ５１）。この結果、他セキュリティポリシ管理装置にセキュリティポリシを管理されている機器との通信要求が含まれている場合（ＮＧ）、その管理装置２０００を特定し、特定した管理装置２０００のセキュリティポリシ連結部２００１に対して、セキュリティポリシ連結部１４からセキュリティポリシの問い合わせを行う（Ｓ５２）。

【００４０】これとは別に、通信要求がセキュリティポリシ管理装置１０００のセキュリティポリシの範囲内でポリシ構成要素管理部３２で行う（Ｓ５３）。セキュリティポリシ管理装置１０００で通信要求がセキュリティポリシの範囲内であることが確認され、同時に、セキュリティポリシ管理装置２０００でも通信要求がセキュリティポリシの範囲内であることが確認され（ＯＫ）、その結果をセキュリティポリシ管理装置１０００が受け取った場合は、機器設定処理を行う（Ｓ５４）。また、いずれか一方のセキュリティポリシ管理装置でセキュリティポリシに合わない通信要求である（ＮＧ）ことが明らかになった場合には、そこで通信要求を実現するための処理は中断し、通信要求を出したネットワーク利用者に対してメッセージで通知して（Ｓ５５）処理を終了する。

【００４１】前記機器設定処理（Ｓ５４）では、セキュリティポリシ管理装置１０００の管理対象範囲に存在する要求された通信を実現するために必要なネットワーク機器、ソフトウェア等を、論理閉域網生成手段検索部２２が、セキュリティポリシ構成要素管理部３２から検索する（Ｓ５６）。この検索結果が、単数の場合（ＯＫ）は、その結果を用い、複数の場合（ＯＫ）は、論理閉域網生成手段選択部２３において、生成手段を登録時に手段毎に付与しておいたツールの評価項目、例えば、セキュリティ強度等を利用して一種類に絞込んだ結果を用い、セキュリティ保護ツール設定チェック部２４が、セキュリティ保護ツール構成要素管理部３３で、その時点の機器設定情報を収集し、その設定状態と矛盾がなければ、第３のインターフェース（ネットワーク機器制御インタフェース）１３から機器設定エージェント４１に設定情報を渡して、機器設定エージェント４１が必要な機器の設定処理を行うと共に、設定した情報を論理閉域網構成要素管理部３１及びセキュリティ保護ツール構成要素管理部３３に保存する。

【００４２】次に、セキュリティポリシ管理装置２０００の管理対象範囲に属する機器との通信が必要な場合（ＮＧ）には、セキュリティ保護ツール設定チェック部２４が、セキュリティポリシ連結部１４から、セキュリティポリシ連結部２００１へ機器設定依頼を通知する（Ｓ５７）。セキュリティポリシ管理装置２０００は、この設定依頼を受け、セキュリティポリシ管理装置２０００の管理範囲内にあるネットワーク機器、ソフトウェア等に設定処理を行って通信要求処理と機器設定処理を終了する。

【００４３】前記通信要求チェック部２１の処理は、図６に示すように、まず、通信要求の種別は、論理閉域網の変更又は削除であるかをチェックする（Ｓ６０）。この結果、通信要求の種別が論理閉域網の変更又は削除であった場合は、論理閉域網構成要素管理部３１から論理閉域網情報を取得する（Ｓ６１）。次に、通信要求に含まれる通信要求範囲をチェックする（Ｓ６２）。そのチェック結果、通信要求自装置管理対象範囲内であれ

ば、自装置のセキュリティポリシの検索を行い（Ｓ６３）、通信要求が自装置管理対象範囲外にも跨る場合は、セキュリティポリシ連結処理を行い（Ｓ６４）、次のステップＳ６５に移る。ステップＳ６５では通信要求がセキュリティポリシの範囲内にあるかをチェックし、前記通信要求がセキュリティポリシの範囲内にあれば（ＯＫ）、機器設定処理を行い（Ｓ６６）、前記通信要求がセキュリティポリシの範囲外にあれば（ＮＧ）、通信要求の否決をユーザに通知して（Ｓ６７）、通信要求チェックの処理は終了する。

【００４４】前記セキュリティポリシ連結の処理は、図７に示すように、他のセキュリティポリシ管理装置２０００を特定し（Ｓ７１）、通信要求内容を他のセキュリティポリシ管理装置２０００へ通知する（Ｓ７２）。次に、セキュリティポリシチェック結果を受信し（Ｓ７３）、セキュリティポリシ連結の処理を終了する。

【００４５】前記機器設定処理は、図８に示すように、論理閉域網生成手段を検索し（Ｓ８１）、この検索された論理閉域網生成手段のうちから所定の論理閉域網生成手段を選択し（Ｓ８２）、その選択された論理閉域網生成手段は、設定に矛盾しないかチェックする（Ｓ８３）。設定に矛盾しない（ＯＫ）時は、機器設定エージェントによる機器の設定を行い（Ｓ８４）、その機器設定情報の保存を行う（Ｓ８５）。設定に矛盾がある（ＮＧ）時は、矛盾発生のメッセージを表示し（Ｓ８８）、機器設定処理は終了する。

【００４６】次のステップＳ８６で通信要求範囲のチェックを行い、前記通信要求が自装置管理対象範囲外にあれば、他装置への機器の設定依頼し（Ｓ８７）、前記機器設定情報が自装置管理対象範囲内にあれば、機器設定処理は終了する。

【００４７】前記論理閉域網生成手段の検索処理は、図９に示すように、通信要求に含まれる端末を導出し（Ｓ９１）、その導出された端末に許可されている手段を検索し（Ｓ９２）、論理閉域網生成手段の検索処理は終了する。

【００４８】前記論理閉域網生成手段の選択処理は、図１０に示すように、論理閉域網生成手段の選択し（Ｓ１０１）、選択された論理閉域網生成手段は複数かをチェックし（Ｓ１０２）、複数であれば（Ｙｅｓ）、論理閉域網生成手段毎に登録されている評価項目から最良の手段を選択して（Ｓ１０３）、論理閉域網生成手段を選択する（Ｓ１０４）。前記選択された論理閉域網生成手段に基づいて論理閉域網を構築することができる。つまり、従来通りにセキュリティポリシを保った論理閉域網を作り出すことができる。

【００４９】図１は、本発明による一実施形態のネットワーク機器等の管理装置の概略構成を示すブロック構成図である。図１において、１００はサービスリモート管理サーバ、１０１はユーザ情報を保存しているユーザ情報データベース（利用者登録データベース）、１０２はネットワーク構成情報を保存しているネットワーク構成情報データベース、１０３は課金方法、決済方法及びサービスに対する課金の情報を保存している課金情報データベース、１０４は利用者のセキュリティポリシ情報を保存しているセキュリティポリシ情報データベース、１０５はユーザ情報管理部、１０６はセキュリティポリシ管理部、１０７はネットワーク利用者の使っているネットワークの情報を保存しているネットワーク構成情報管理部、１０８はネットワーク利用者から送信されてきた通信要求の可否を判別する通信要求判別部、１０９は通信要求を満たすために必要な具体的なネットワーク機器等の設定を導出するセキュリティ保護ツール設定管理部、１１０はネットワーク利用者から通信要求が送られて来たときに課金処理を行う課金処理部、２００はリモート管理サービスサーバとネットワーク利用者が使用中のネットワークを結ぶネットワーク（例えばインターネット）、３００はネットワーク利用者が使用中の個別のクライアント、４００はネットワーク利用者が使用中のネットワークと外部のネットワークとの接続を制御しているファイアウォール、４０２は一つ以上のネットワーク利用者をまとめて管理するためのグループＩＤである。

【００５０】本実施形態のネットワーク機器等の管理装置は、図１に示すように、サービスリモート管理サーバ１００と、リモート管理サービスサーバとネットワーク利用者が使用中のネットワークを結ぶネットワーク（例えばインターネット）２００と、ネットワーク利用者が使用中の個別のクライアント３００と、ネットワーク利用者が使用中のネットワークと外部のネットワークとの接続を制御しているファイアウォール４００とで構成されている。

【００５１】前記サービスリモート管理サーバ１００は、利用者の情報を保存しているユーザ情報データベース（利用者登録データベース）１０１、ネットワーク構成情報を保存しているネットワーク構成情報データベース１０２、課金方法、決済方法及びサービスに対する課金の情報を保存している課金情報データベース１０３、別のセキュリティポリシ管理装置からの利用者のセキュリティポリシ情報を保しているセキュリティポリシ情報データベース１０４、前記ユーザ情報データベース１０１からのユーザ（利用者）情報の管理を行うユーザ情報管理部１０５、前記利用者のセキュリティポリシ情報の管理を行うセキュリティポリシ管理部１０６、ネットワーク利用者の使っているネットワークの情報を保存しているネットワーク構成情報管理部１０７、ネットワーク利用者から送信されてきた通信要求の可否を判別する通信要求判別部１０８、通信要求を満たすために必要な具体的なネットワーク機器等の設定を導出するセキュリティ保護ツール設定管理部１０９及びネットワーク利用者

から通信要求が送られて来たときに課金処理を行う課金処理部１１０を有している。

【００５２】前記ネットワーク利用者が使用中の個別のクライアント３００には、セキュリティ保護ツール３０１と利用者ＩＤ３０２を有している。前記ファイアウォール４００は、ネットワーク利用者が使用中のネットワークと外部のネットワークとの接続を制御する。このファイアウォール４００にはグループＩＤ４０２が入力される。前記グループＩＤ４０２は、複数のクライアントの利用者ＩＤ４０３をまとめた識別子である。

【００５３】図１１は、図１のネットワーク機器等の管理装置における、ネットワーク管理委託処理手順の全体を示す流れ図である。まず、利用者が登録情報をユーザ情報管理部１０５に送信し、その結果をユーザ情報データベース（利用者登録データベース）１０１に登録（保存）し（Ｓ１０１）、利用者登録が済んでからセキュリティポリシをセキュリティポリシ管理部１０６（図２参照）に送信し、この送信されてきたセキュリティポリシをセキュリティポリシ情報データベース１０４に登録（保存）する（Ｓ１０２）。この状態になると、ネットワーク利用者から通信要求を受け付けることができるようになる（Ｓ１０３）。前記ステップＳ１０２、Ｓ１０３を繰り返しネットワーク管理の委託サービスを続けることができる。また、セキュリティポリシの変更がある際には、セキュリティポリシ管理部１０６でセキュリティポリシの変更処理を行ってセキュリティポリシ情報データベース１０４の内容を変更することもできる（図２、図６参照）。

【００５４】図１２は、利用者登録処理の手順を示す流れ図である。利用者登録処理には、ネットワーク情報の登録があり、どのクライアント３００に何のセキュリティ保護ツール３０１が装備されているのか、どのファイアウォール４００に何の機能が装備されているのか、といった内容をネットワーク構成情報管理部１０７に通知し、ネットワーク構成情報管理部１０７はネットワーク構成情報データベース１０２に登録（保存）する（Ｓ２０１）。次に、利用者登録しようとしている利用者は、課金方法と決済方法をユーザ情報管理部１０５に送信し、ユーザ情報管理部１０５ではその選択された課金方法（Ｓ２０２）と決済方法を課金情報データベース１０３に登録する（Ｓ２０３）と共に、ユーザ情報データベース１０１を参照し既存の利用者と一意に区別できる利用者ＩＤ３０２及びグループＩＤを生成した後に利用者に通知し（Ｓ２０４）、それらのＩＤ情報をユーザ情報データベース１０１に登録（保存）する。また、利用者には、様々な権限を表す属性を付与することができ、利用者が希望する場合には、その属性もユーザ情報データベース１０１に登録（保存）する。この属性には、例えば、通信要求を出すことができるユーザに付与する属性や変更も行うことができるユーザに付与する属性等がある。

【００５５】図１３は、セキュリティポリシ登録・変更処理の手順を示す流れ図である。セキュリティポリシ登録・変更処理では、ユーザはクライアント３００からセキュリティポリシをセキュリティポリシ管理部１０６に送信し、セキュリティポリシ管理部１０６では送信されてきたセキュリティポリシを受け付け（Ｓ３０１）、その受け付けたセキュリティポリシについて、そのユーザに関するセキュリティポリシ全体としての整合性をチェックし（Ｓ３０２）、そのチェックで整合性が保たれていることが確認される（図２参照）と、セキュリティポリシ情報データベース１０４に登録（保存）する（Ｓ３０４）。

【００５６】図１４は、通信要求受付処理の手順を示す流れ図である。通信要求受付処理は、通信要求判別部１０８がネットワーク利用者からの通信要求を受け付けることから始まる（Ｓ４０１）。次に、図１５に示す利用者権限チェック処理を行う（Ｓ４０２）。ここでは、まず、通信要求受付処理がネットワーク利用者から受け取った通信要求に含まれているグループＩＤやユーザＩＤとユーザ情報データベース１０１を使い、通信要求を送信する権限があるユーザからの通信要求であるか否かをチェックする（Ｓ５０１）。この結果、通信要求を出す権限を持った利用者からの通信要求であることが確認できれば（Ｙｅｓ）、次に、課金情報データベース１０３を使い課金方法のチェックを行う（Ｓ５０２）。また、権限があることが確認できない場合（Ｓ５０１のＮｏ）にはサービスを拒否する（Ｓ５０５）。ここでは、通信要求を送信してきた利用者が課金情報データベース１０３に登録している課金方法から、従量制課金を選択しているか定額制課金を選択しているかを調べ、従量制課金を選択している場合は、通信要求に基づくサービスを提供した後に課金するための情報を一時的に保持する（Ｓ５０３）。課金方法がいずれの場合でも、さらに課金情報データベース１０３を使い料金の滞納があるか否かを調べ（Ｓ５０４）、滞納があれば（Ｎｏ）、サービスを拒否し（Ｓ５０５）、滞納が無ければ（Ｙｅｓ）、利用者権限チェックを終了する。

【００５７】図１６は、通信要求反映処理の手順を示す流れ図である。まず、通信要求判別部１０８が受信した通信要求が、事前に登録されているセキュリティポリシ情報データベース１０４に合致しているか否かを判断する（Ｓ６０１）。通信要求判別部１０８は、合致していない場合（Ｎｏ）はサービスを中止し（Ｓ６０７）、合致している場合は通信要求を実現するために設定しなければならないネットワーク機器などをネットワーク構成情報データベース１０２を用いて導出する（Ｓ６０３）。

【００５８】セキュリティ保護ツール設定管理部１０９

は、通信要求判別部１０８が設定対象として導出した機器、ソフトウェア等の設定内容を個別に導出し、導出した設定内容をネットワーク機器、ソフトウェア等に対して設定する指示を与える（Ｓ６０４）。通信要求やネットワーク構成によって設定対象や内容は変化するが、例えば、３００クライアントのように、クライアント自身にセキュリティ保護ツール３０１が実装されている場合には、そのツールの設定を変更し、クライアントが保持している利用者ＩＤに対して課金処理を行うような形態もあれば、クライアントの利用者ＩＤ４０３が通信要求を送信した結果、外部ネットワークとの接続機器であるファイアウォール４００に具備されているセキュリティ保護ツール４０１の設定を変更した後に、通信要求を送信したクライアントの利用者ＩＤ４０３が含まれるグループＩＤ４０２に課金する形態もあり得る。

【００５９】このような設定が終わった後、課金方法を調べて（Ｓ６０５）、一時的に保存していた情報を基に、課金処理部１１０が課金処理を実施する（Ｓ６０６）。

【００６０】図１７は、通信要求を送信するクライアントで行われる通信要求送信処理の手順を示す流れ図である。クライアント３００では通信要求の送信を行うソフトウェアで通信要求を入力し（Ｓ７０１）、利用者登録をした際の課金形態に対応する利用者ＩＤ又はグループＩＤを入力した通信要求に付加し（Ｓ７０２、Ｓ７０３、Ｓ７０４）、サービスリモート管理サーバ１００へ通信要求とＩＤを送信する（Ｓ７０５）。

【００６１】図１８は、本サービスを利用する際に利用できるグループ課金の処理を簡略化する包含関係ＩＤを示す図である。利用者ＩＤは、ネットワーク利用者が通信要求を前記管理装置に送信するクライアント３００に対して付与されている。利用者がクライアント３００を移動することを考慮して、クライアント３００へのログイン時に付与することも可能であり、特定のハードウェアに固定的に付与することも可能である。また、グループＩＤは、一つ以上の利用者ＩＤの集合に対して付与される。前記図１の本実施形態では特定のサブネットに属する利用者に付与されたＩＤの集合を表すＩＤとして定義している。ネットワーク利用者単位課金の場合には利用者ＩＤ、グループ単位課金の場合には利用者ＩＤまたはグループＩＤのいずれか一方を通信要求に付与する。

【００６２】利用者ＩＤとグループＩＤとの対応関係は、その対応情報を通信要求の受信者である前記管理装置が保持するか、包含関係を表すＩＤ体系を利用して表す。前者は、利用者ＩＤとグループＩＤの対応関係を表す情報をサーバで保持する必要があるが、以下に説明する包含関係ＩＤではそれが不要になる。包含関係ＩＤとは、二桁以上からなる数値を固定的な桁数で分割して認識するルールをＩＤの送信者と受信者が予め決めておくことによって、利用者とグループの特定情報が交換できるものでる。図１８では、「０００」という値を利用者個別ＩＤに利用せず、「０００」がついている場合にはグループＩＤを表すというルールにしておくことによって、包含関係ＩＤが達成されている。

【００６３】なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。

【００６４】また、「コンピュータ読み取り可能な記録媒体」とは、フロッピー（登録商標）ディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の記録媒体、コンピュータシステムに内蔵されるハードディスク等の記録装置をいう。

【００６５】以上、本発明者によってなされた発明を、前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【００６６】

【発明の効果】以上説明したように、本発明によれば、ネットワーク利用者が論理閉域網を要求してから、人による作業を介することなく、論理閉域を使えるようになるので、人を介した論理閉域網の管理サービスに比べて時間を短縮することができる。

【００６７】また、包含関係ＩＤを利用することによって、サービス提供側で利用者ＩＤとグループＩＤというような複数種類のＩＤの対応関係を表す情報を保持する必要がなくなる。

【００６８】また、ネットワーク機器、ソフトウェア等の管理を行うネットワーク機器等の管理方法及び装置において、ネットワーク機器、ソフトウェア等の管理を委託された側で委託した作業を行い、委託した側から対価を得ることができる。

【図面の簡単な説明】

【図１】本発明による一実施形態のネットワーク機器等の管理装置の概略構成を示すブロック構成図である。

【図２】本発明に係る一実施形態のコンピュータシステムからなるセキュリティポリシ管理装置の概略構成を示すブロック構成図である。

【図３】図２に示すセキュリティポリシ管理の処理手順を示す流れ図である。

【図４】図２に示す機器設定処理の処理手順を示す流れ図である。

【図５】図３に示す通信要求処理手順を示す流れ図である。

【図６】本実施形態の通信要求チェック部の処理手順を示す流れ図である。

【図７】本実施形態のセキュリティポリシ連結の処理手順を示す流れ図である。

【図８】本実施形態の機器設定処理の手順を示す流れ図

である。

【図９】本実施形態の論理閉域網生成手段の検索処理手順を示す流れ図である。

【図１０】本実施形態の論理閉域網生成手段の選択処理手順を示す流れ図である。

【図１１】本実施形態のネットワーク管理委託処理手順の全体を示す流れ図である。

【図１２】本実施形態の利用者登録の処理手順を示す流れ図である。

【図１３】本実施形態のセキュリティポリシ登録・変更処理手順を示す流れ図である。

【図１４】本実施形態の通信要求受付処理手順を示す流れ図である。

【図１５】本実施形態の利用者権限チェック処理手順を示す流れ図である。

【図１６】本実施形態の通信要求反映処理手順を示す流れ図である。

【図１７】本実施形態の通信要求送信処理手順を示す流れ図である。

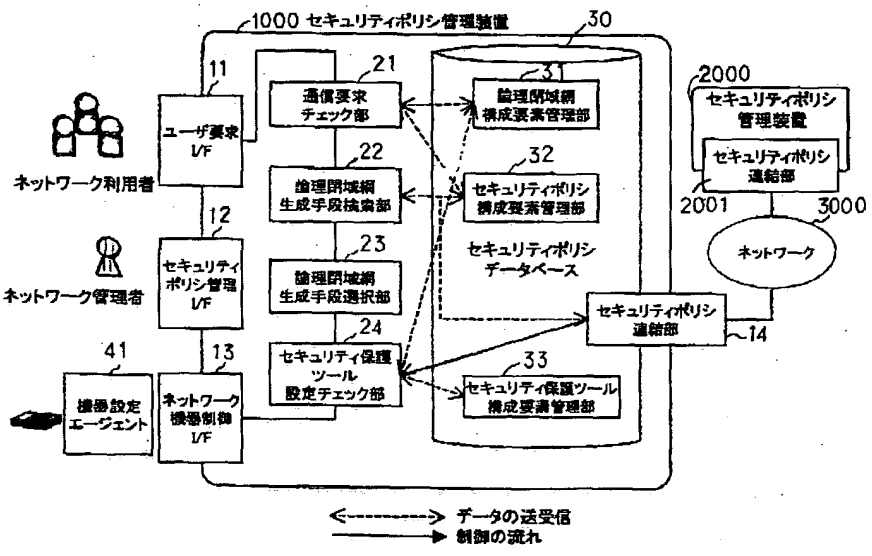
【図１８】本実施形態の包含関係ＩＤの例を示す図である。

【符号の説明】

１１…第１のインタフェース
１２…第２のインタフェース
１３…第３のインタフェース
１４…セキュリティポリシ連結部
２１…通信要求チェック部
２２…論理閉域網生成手段検索部
２３…論理閉域網生成手段選択部
２４…セキュリティ保護ツール設定チェック部
３０…セキュリティポリシデータベース
３１…論理閉域網構成要素管理部
３２…セキュリティポリシ構成要素管理部
３３…セキュリティ保護ツール構成要素管理部
４１…機器設定エージェント
１０００…セキュリティポリシ管理装置
２０００…セキュリティポリシ管理装置
２００１…セキュリティポリシ連結部
１００…サービスリモート管理サーバ
１０１…ユーザ情報データベース
１０２…ネットワーク構成情報データベース
１０３…課金情報データベース
１０４…セキュリティポリシ情報データベース
１０５…ユーザ情報管理部
１０６…セキュリティポリシ管理部
１０７…ネットワーク構成情報管理部
１０８…通信要求判別部
１０９…セキュリティ保護ツール設定管理部
１１０…課金処理部
２００…ネットワーク
３００…クライアント
３０１…セキュリティ保護ツール
３０２…利用者ＩＤ
４００…ファイアウォール
４０１…セキュリティ保護ツール
４０２…グループＩＤ
４０３…クライアントの利用者ＩＤ

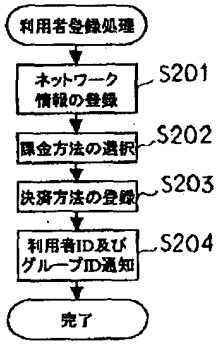
【図２】

図２



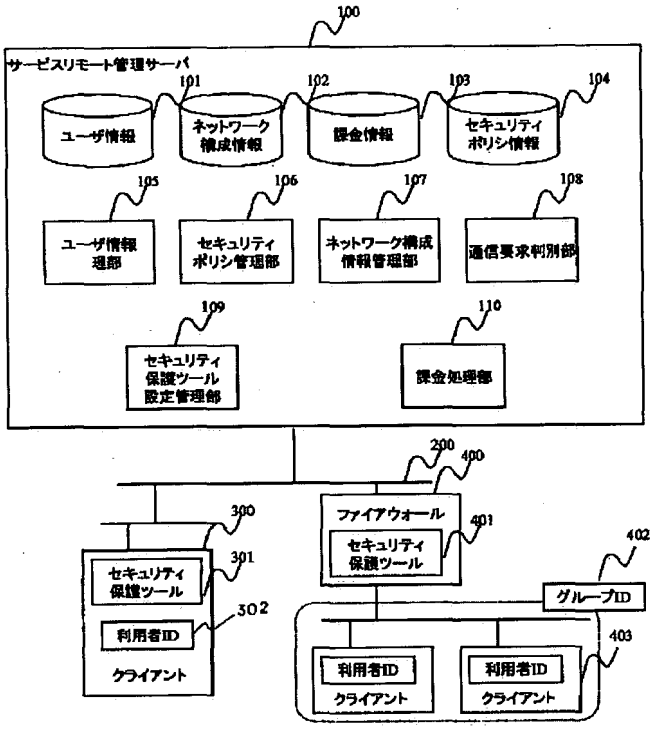
【図１２】

図１２



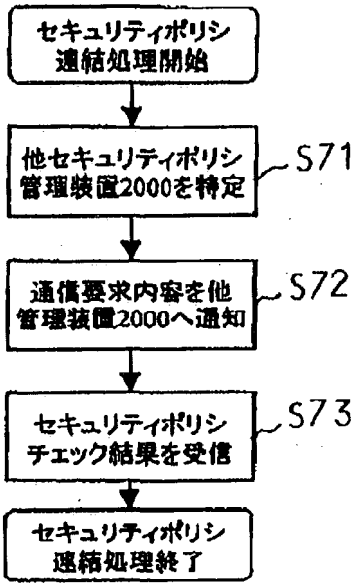
【図１】

図１



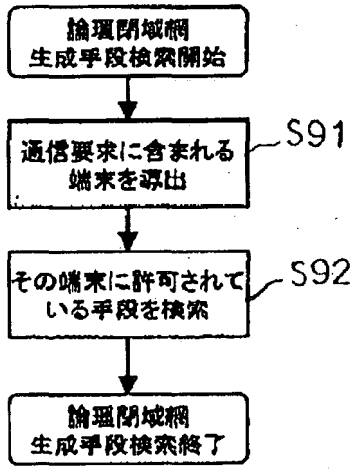
【図７】

図７



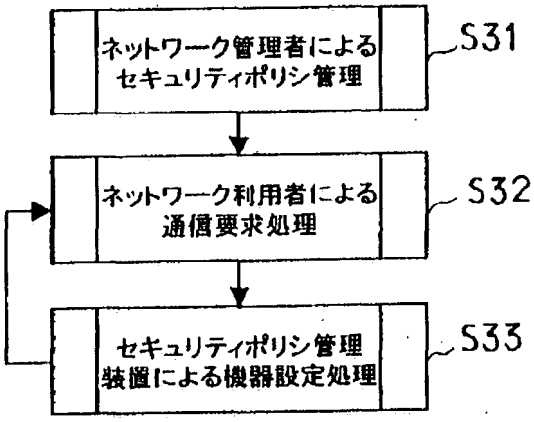
【図９】

図９



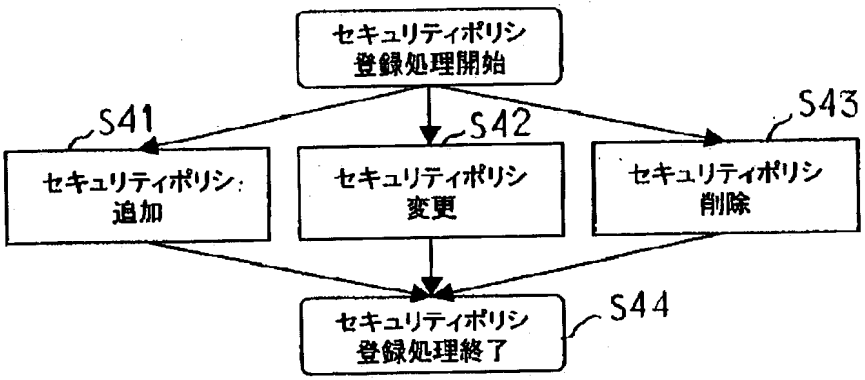
【図３】

図３



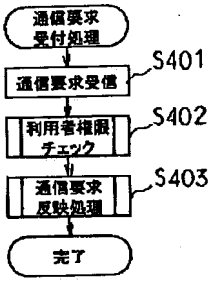
【図４】

図４



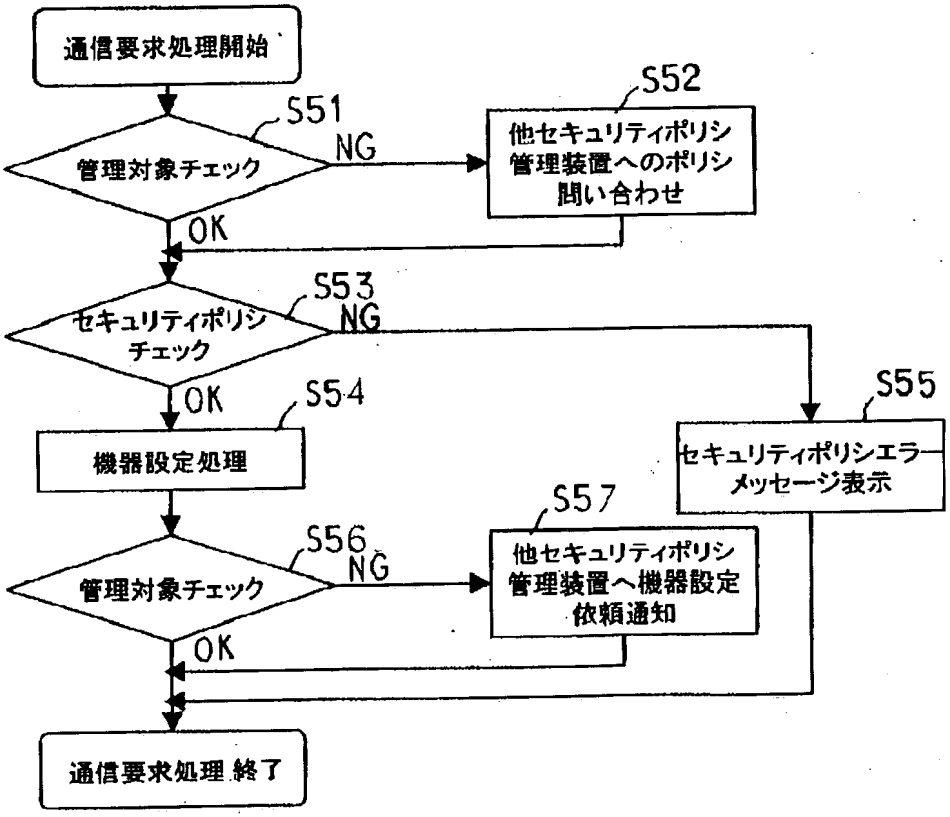
【図１４】

図１４



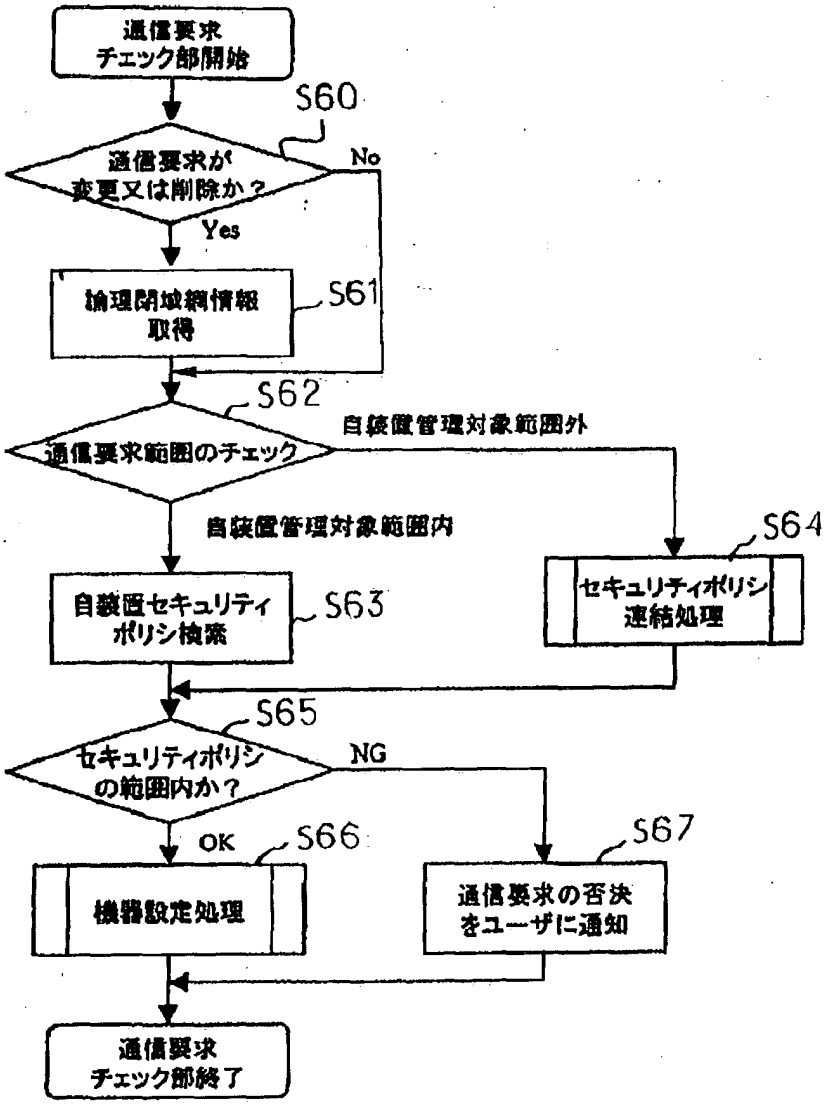
【図５】

図５



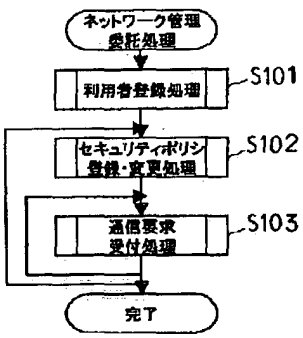
【図６】

図６



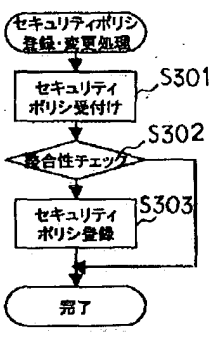
【図１１】

図１１



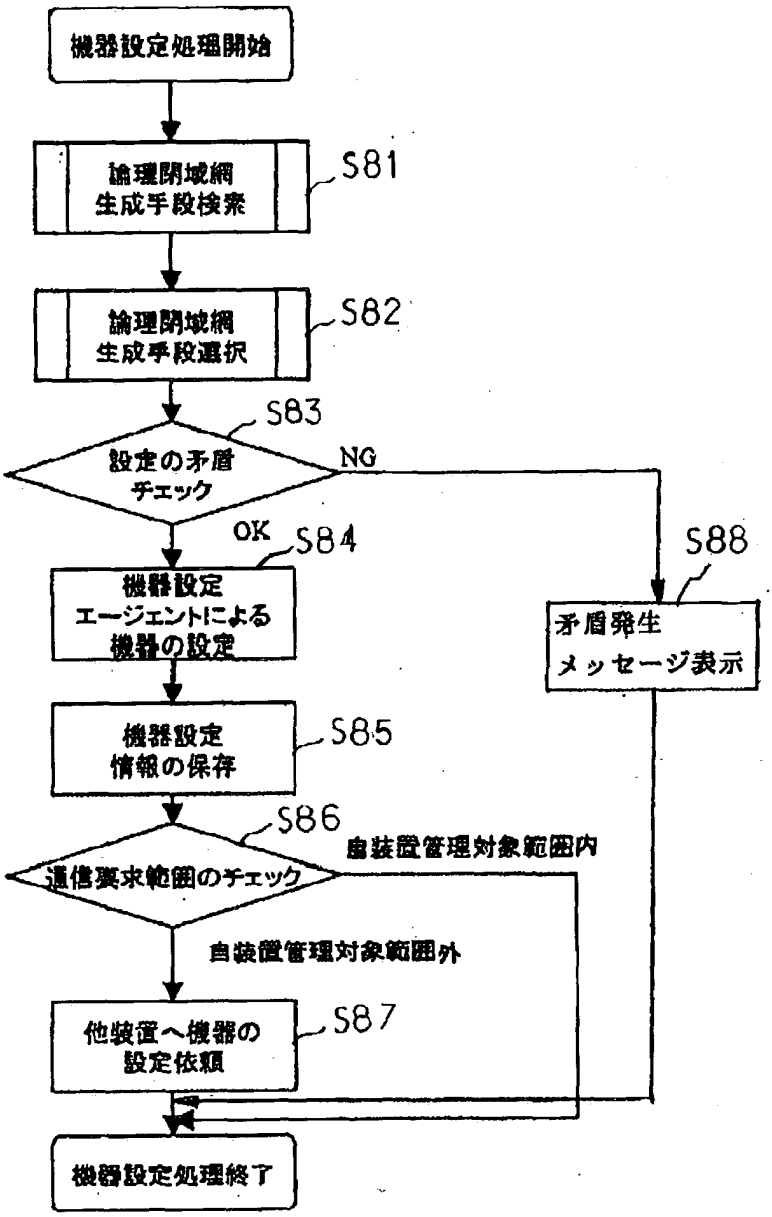
【図１３】

図１３



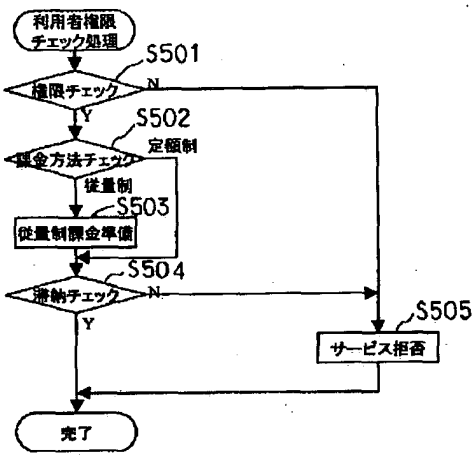
【図８】

図８



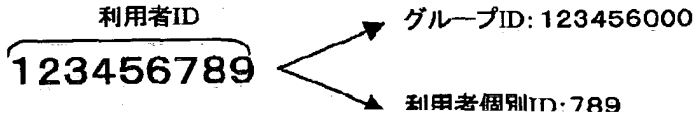
【図１５】

図１５



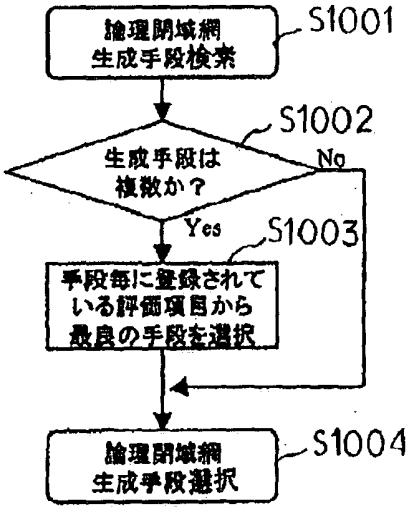
【図１８】

図１８



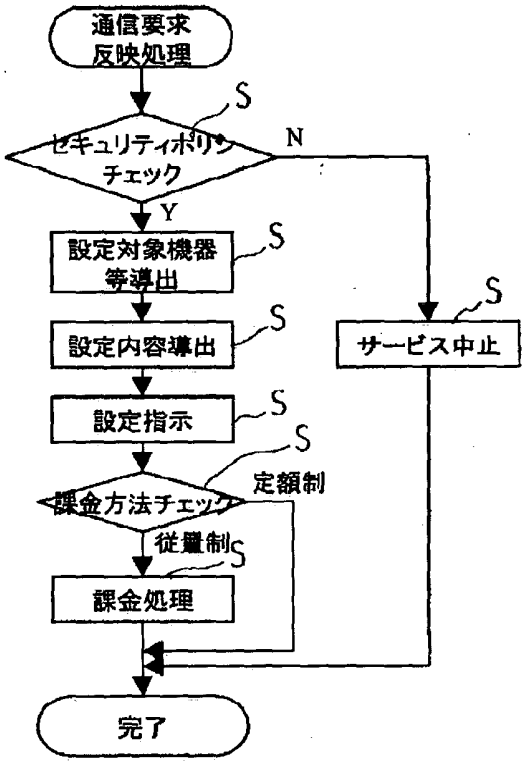
【図１０】

図１０



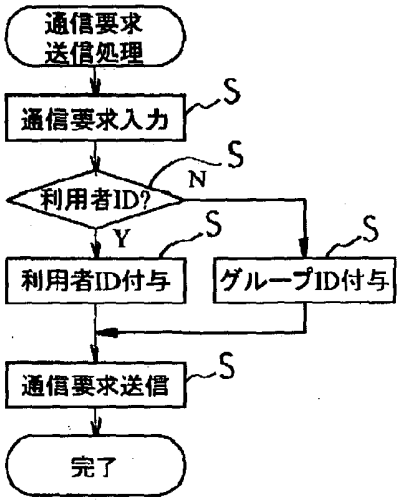
【図１６】

図１６



【図１７】

図１７



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
Ｈ０４Ｌ	12/28		Ｈ０４Ｌ	11/20	１０２Ｄ
	12/56				
// Ｇ０６Ｆ	17/60	３３２			